情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

MPEG-2 스트리밍 DRM 시스템 설계 및 구현

정 연 정, 윤 기 송, 류 재 철*

요 약

본 논문은 MPEG-2 스트리밍 콘텐츠에 대한 보호와 사용권한을 관리하는 DRM 시스템을 제안한다. 본 논문은 스트리밍 콘텐츠에 대한 암호화를 통하여 콘텐츠를 보호하고 사용자에게 스트리밍 서비스에 대한 권리와 암호화된 스트리밍 콘텐츠를 복호화하기 위한 키를 안전하게 전달하기 위한 저작권 관리 방법을 제안한다. 본 논문에서 제안하는 MPEG-2 암호화 방안은 암호화된 MPEG-2 스트리밍 콘텐츠가 스트리밍 서버의 성능에 영향을 미치지 않도록 하며 DRM 적용으로 인한 스트리밍 클라이언트에서의 부하가 최소화될 수 있도록 한다.

Ⅰ. 서 론

오늘날 새로운 디지털 콘텐츠에 대한 제작이 용이하고 인터넷을 통한 사용이 쉽게 이루어지고 있다. 즉, 디지털 기술의 발전에 따라 텍스트, 이미지, 오디오, 비디오, 게임 등 다양한 종류의 콘텐츠가 효과적으로 생산되고 배포되고 있으며, 네트워크 기술의 발전에 따라 스트리밍 콘텐츠를 각 가정에 까지 실시간으로 스트리밍 서비스할 수 있는 단계에 있다.

현재의 콘텐츠 스트리밍 서비스 모델은 ID/Password와 같은 간단한 인증을 통한 접근 권한 관리에 의존하고 있으며 이러한 방법은 근본적인 콘텐츠에 대한 보호 방법을 제공하지 못하고 있다. 즉, 넷트워크 패킷 캡쳐나 스트리밍 URL 캡쳐와 같이 해킹 툴을 이용한 불법 콘텐츠 유통을 방지하는데 한계가 있다[10,12].

최근 Microsoft, Widevine, Verimatrix 등에서 스트리밍 컨텐츠를 보호할 수 있는 DRM 기반의 콘텐츠 보호 방법이 제시되고 있으며, 국내에서는 실트로닉스, 코아트러스트 등에서 스트리밍 콘텐츠를 보호할 수 있는 방안이 제시되고 있는 상태이다.

DRM을 이용한 다운로드형의 콘텐츠 보호하는 방법은 기존의 콘텐츠 보호 방법과 비교해 효과적인 콘텐츠 보호 방법을 제시하고 있다. DRM 기반의 다운로드형의 콘텐츠 보호는 콘텐츠 전체를 암호화하고 사용자에게 전달한 후 라이센스 발행 프로토콜에 따라 안전한 콘텐츠 유통 방법을 제공한다.

그러나, 스트리밍 콘텐츠에 대한 보호는 다운로드 형의 콘텐츠 보호와는 달리 실시간으로 콘텐츠 제공해야 하는 특성과 스트리밍 서버가 스트리밍 서비스를 제공하는데 필요한 데이터가 콘텐츠 내에 존재하는 특성이 있다. 다운로드형 콘텐츠와 같이 스트리밍 콘텐츠 전체를 암호화 한다면 스트리밍 서버는 콘텐츠 내에 존재하는 스트리밍 정보를 얻을 수 없기 때문에 스트리밍 서비스를 할 수 없으며, 스트리밍 시 패킷에 대한 암호화를 수행 한다면 서버에 대해 과중한 부하를 일으키게 된다.

본 논문은 스트리밍 서버의 환경과 스트리밍 프로토콜에 영향을 주지 않으면서 스트리밍 콘텐츠를 안전하게 사용자에게 서비스할 수 있는 DRM을 기반으로 한 MPEG-2 스트리밍 콘텐츠에 대한 보호 방안을 제안한다. MPEG-2 스트리밍 콘텐츠에 대한 암호화를 통하여 콘텐츠를 보호하고, MPEG-2 콘텐츠에 대한 암호화 키와 사용권한을 라이센스를 통하여 전달하여 정당한 사용자만이 스트리밍 서비스를 받을 수 있도록 하여 콘텐트 유통 밸류 체인(Value-Chain)에 참여하는 유통 주체의 권리를 보호한다.

본 논문의 구성은 제 2장에서 MPEG-2 TS 보호 방법에 대해서 살펴보고, 제3장에서 제안된 시스템의 구조와 기능에 대해서 알아보고, 제 4장에서 결론 및 향후 연구에 대해서 알아본다.

* 충남대학교 (jcryou@home.cnu.ac.kr)

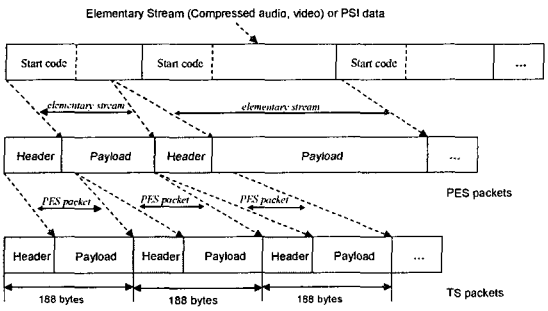
II. MPEG-2 TS 보호 방법

1. MPEG-2 TS 비디오 암호화 방법

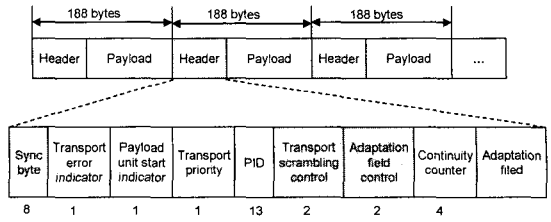
MPEG은 비디오와 오디오를 압축하기 위한 표준이며 비디오와 오디오 Elementary stream을 저장 또는 전송하기 위해 패킷화하는 과정으로 저장매체에 저장하기 위한 프로그램 스트림(Program Stream, PS)과 네트워크로 전송하기 위한 트랜스포트 스트림(Transport Stream, TS)이 있다. TS는 모든 Elementary stream을 하나의 전송 스트림으로 전송하기에 적합하도록 인코딩하기 위해 고안되었으며[14] TS 스트림은 일련의 TS 패킷으로 구성되는데 TS 패킷들은 각각의 길이가 188 바이트이다. 그림 1에서 TS를 구성하기 위한 MPEG-2 레이어 구성을 볼 수 있다.

본 논문에서 제안하는 비디오 TS 암호화 방안은 Elementary stream의 I-프레임 데이터를 포함하는 TS 패킷을 암호화한다. Elementary stream의 I-프레임 데이터를 포함하는 비디오 TS 패킷의 Payload를 암호화하는 이유는 두 가지가 있는데, 첫째 스트리밍 서버가 TS 파일을 인스톨할 때 PAT(Programme Association Table), PMT(Programme Map Table), SEQ Header(Sequence Header), VCR 기능을 지원하기 위한 Index 파일을 생성할 때TS/PES/Elementary stream의 메타데이터가 스트리밍 서버에 의해 사용되기 때문이다. 둘째 암호화되는 데이터 양을 줄이기 위해서 인데, I, B, P-프레임의 모든 프레임 데이터를 암호화할 수도 있지만 B-프레임과 P-프레임은 I-프레임이 없이 원래 이미지를 생성하는 것이 어렵기 때문에 I-프레임의 데이터를 암호화하는 것만으로 스트리밍 콘텐츠를 보하는 것이 가능하다.

비디오 TS 패킷의 Payload는 Elementary stream에 존재하는 비디오 시퀀스(Sequence) 정보를 포함하는데, 이 정보를 이용하여 어떤 비디오 TS 패킷이



〔그림 1〕 MPEG-2 레이어 구성도



〔그림 2〕 MPEG-2 TS 패킷 헤더 구조

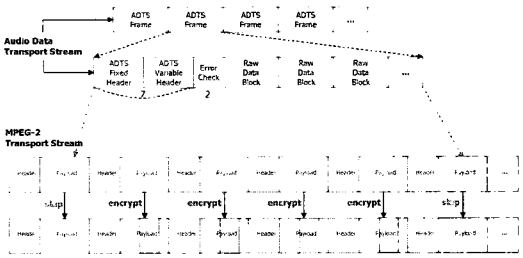
I-frame의 영역에 포함되는지 알 수 있다. 즉, 비디오 스트림 PID를 포함하는 TS 패킷의 Playload 내에서 I-프레임의 시작을 알리는 start code와 I-프레임 이외의 시작을 알리는 start code를 알 수 있다. I-프레임 데이터를 암호화는 비디오 TS 패킷의 Payload에서 I-프레임의 start code가 존재하는 비디오 TS 패킷부터 다른 start code를 포함하는 비디오 TS 패킷이 나타나기 이전까지의 모든 비디오 TS 패킷의 Payload에 있는 I-프레임 데이터를 암호화한다.

본 논문에서는 TS 패킷이 암호화되었다는 것을 구분하기 위해 암호화된 TS 패킷의 transport scrambling control bits의 값을 '11'로 변경한다. TS 패킷의 transport scrambling control bits의 기본 값은 '00'이다. DRM 클라이언트는 이 값을 이용하여 TS 패킷이 암호화되었는지를 판별하게 되는데, TS 패킷의 transport scrambling control bits의 값이 '11'인 TS 패킷만 복호화 한다.

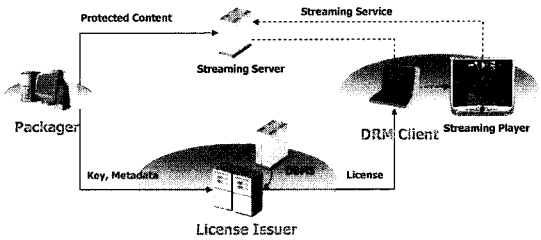
2. MPEG-2 TS 오디오 암호화 방법

MPEG-2 오디오 Elementary stream의 형식인 ADTS(Audio Data Transport Stream)은 파일 헤더가 없고 ADTS 프레임들로 구성되어 있다. ADTS 프레임은 헤더 (7 바이트), CRC(2 바이트), 데이터 블록으로 구성되어 있다. 프레임의 헤더는 고정 헤더와 가변 헤더로 이루어져 있는데, 고정 헤더는 모든 프레임이 같은 값을 가지고 있으나 가변 헤더는 다른 값을 가질 수 있다. 각 프레임의 시작은 첫 12 비트 코드로 알 수 있는데, 'syncword'라 부르며 '0xFFF'의 값을 가진다.

본 논문에서 제안하는 오디오 암호화 방안은 Elementary stream의 오디오 프레임 데이터를 포함하는 오디오 TS 패킷만을 암호화한다. 오디오 스트림 PID를 포함하는 TS 패킷의 Payload를 검사하여 syncword를 찾아내어 TS 패킷의 Payload에 존재하는 오디오 프레임 데이터를 암호화하기 시작하여 다음 syncword를 포함하는 오디오 TS 패킷을 찾을 때까지 TS 패킷의



〔그림 3〕 MPEG-2 오디오 암호화



〔그림 4〕 MPEG-2 스트리밍 DRM 시스템 구성도

Payload에 존재하는 오디오 프레임 데이터에 대한 암호화를 진행한다.

MPEG-2 TS 비디오 암호화와 같은 방법으로 오디오 TS 패킷이 암호화되었다는 것을 구분하기 위해 암호화된 TS 패킷의 transport scrambling control bits의 값을 '11'로 변경한다. 그림 3은 오디오 시퀀스 레이어와 오디오 Elementary stream의 암호화된 영역이 TS 패킷의 Payload에 어떻게 매핑되는가를 나타난다.

3. MPEG-2 TS 비디오/오디오 복호화 방법

암호화된 데이터에 대한 복호화는 TS 패킷의 25번째와 26번째 비트에 존재하는 transport scrambling control bits의 값을 검사하여 그 값이 '11'인 경우에 복호화를 수행하고 transport scrambling control bits의 값을 '00'로 변경한다. 만일 TS 패킷의 transport scrambling control bits의 값이 '00'인 경우에는 바이패스(by-pass)된다. 복호화 된 TS 패킷은 원래의 TS 패킷과 동일한 데이터를 가지게 된다.

제안된 복호화 방안은 MPEG-2 TS/PES/Elementary stream의 형식을 분석하지 않고 단지, TS 패킷의 25번째와 26번째 비트에 존재하는 transport scrambling control bits의 값을 검사하는 부하와 TS의 Payload의 암호화된 영역을 복호화하는 부하를 가지게 하여 DRM 클라이언트에서의 부하를 최소화할 수 있도록 한다.

Ⅲ. MPEG-2 스트리밍 DRM 시스템

MPEG-2 스트리밍 DRM 시스템은 패키저, 라이센스 이슈어, DRM 클라이언트로 구성되어 있다. 그림 4는 제안된 시스템의 구성을 보여준다.

시스템을 구성하는 각 서브시스템은 다음과 같은 기능을 가진다. 패키저는 암호키를 생성하여 원본 콘텐츠를 암호화하고 암호화에 관련된 메타데이터를 생성한다.

- 콘텐츠 입력 및 메터데이터 입력/편집
- 콘텐츠 암호화키 생성
- MPEG-2 구조 분석 및 파싱
- DRM-enabled 콘텐츠 생성 (MPEG-2 콘텐츠 암호화, 라이센스 정보 생성)

라이센스 이슈어는 암호키와 메타데이터를 포함하는 라이센스를 생성하고 DRM 클라이언트의 공개키로 라이센스를 암호화하여 DRM 클라이언트로 전송한다.

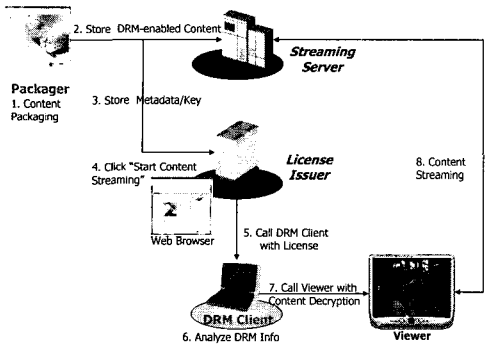
- DB로부터 라이센스 정보(암호화키, 암호화 정보, 플러그인 정보) 추출
- 콘텐츠 암호키를 DRM 클라이언트의 공개키로 암호화
- 암호키, 암호화 정보, 플러그인 정보를 이용하여 라이센스 생성
- DRM 클라이언트에 라이센스 발급

DRM 클라이언트는 라이센스를 수신하여 라이센스를 분석하고 그 정보에 따라 스트리밍되는 콘텐츠를 복호화한다.

- 라이센스를 분석하여 암호화키, 암호화 정보, 플러그인 정보 추출
- DRM 클라이언트의 공개키로 암호화된 콘텐츠 암호키를 복호화
- 콘텐츠 암호화키를 이용하여 스트리밍 콘텐츠 실시간 복호화
- 콘텐츠 플레이어 제어

MPEG-2 스트리밍 DRM 시스템의 수행 흐름은 다음과 같다. 그림 5는 제안된 시스템의 흐름을 보여준다.

1. 패키저가 특정 콘텐츠를 선택하여 패키징한다.
2. 패키징된 콘텐츠를 스트리밍 서버에 저장한다.
3. 라이센스 이슈어 서버에서 라이센스 발행 정보를



〔그림 5〕 MPEG-2 스트리밍 DRM 시스템 흐름도

등록한다.

4. 사용자가 콘텐츠 스트리밍 시작을 클릭한다.
5. 웹브라우저가 해당 콘텐츠의 정보를 읽어 DRM 클라이언트를 호출한다.
6. DRM 클라이언트는 라이센스 정보를 분석한다.
7. Viewer를 실행하며, 스트리밍 콘텐츠를 복호화한다.
8. Viewer가 복호화된 스트리밍 콘텐츠를 사용자에게 보여준다.

본 시스템의 구현은 패키저는 Microsoft Windows 환경의 애플리케이션으로 구현되었으며, 라이센스 이슈어는 Linux RedHat 8.0 환경에서 자바 서블릿으로 구현되었으며, DRM 클라이언트는 Microsoft Windows 환경의 ActiveX로 구현되었다. 스트리밍 서버는 Linux RedHat 8.,0에서 동작하는 Kasenna XMP 7.0을 기반으로 하였으며 스트리밍 플레이어는 Microsoft Windows에서 동작하는 Kasenna Brodband Player를 기반으로 한다.

1. 패키저 (Packager)

본 논문에서는 스트리밍 콘텐츠에 대한 불법적인 사용을 방지하기 위하여 스트리밍 콘텐츠에 대한 암호화를 수행한다. 그런데, 스트리밍 서버가 스트리밍 서비스를 제공하기 위해서는 스트리밍 콘텐츠에 포함된 메타데이터를 이용하기 때문에 스트리밍 콘텐츠가 암호화가 되었다 하더라도 스트리밍 콘텐츠의 포맷이나 메타데이터가 변경되지 않아야 한다. 본 논문은 원본 스트리밍 콘텐츠를 분석하고 암호화될 데이터 영역을 결정하여 데이터 형식 변환 없이 데이터 PAYLOAD 영역을 암호화한다.

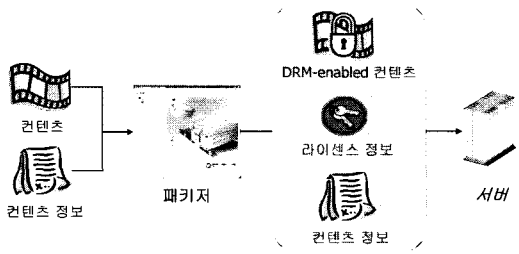
패키저는 원본 스트리밍 콘텐츠로부터 암호화된 스트리밍 콘텐츠와 라이센스를 생성하기 위한 메타데이터를 생성한다. 라이센스를 생성하기 위한 메타데이터는 암호화 키, 암호화 정보(암호화 크기, 암호화 비율), 미디어 종류, 플러그인 정보 등이 있다. 본 논문에서 제안하는 스트리밍 콘텐츠를 암호화하고 암호화된 스트리밍 콘텐츠 자체를 스트리밍하는 방법은 네터워크 상에서 패킷 캡쳐 또는 스트리밍 URL 캡쳐에 의한 누출에 안전할 뿐만 아니라 콘텐츠가 사용자 PC에 다운로드되었다 할 지라도 라이센스가 없으면 재생이 불가능하기 때문에 안전한 스트리밍 서비스를 제공할 수 있다.

스트리밍 콘텐츠의 초당 전송 데이터량은 작게는 몇 메가바이트에서 많게는 20 메가바이트까지 전송되므로 패키저는 클라이언트 시스템의 성능을 고려하여 스트리밍 콘텐츠를 최적으로 복호화할 수 있도록 암호화할 패킷 비율과 암호화할 크기를 조절할 수 있다.

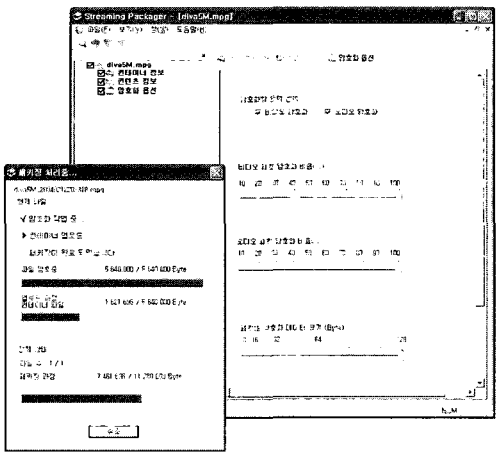
그림 6은 패키저의 데이터 흐름을 보여주고, 그림 7은 패키저의 실행 화면이다.

2. 라이센스 이슈어 (License Issuer)

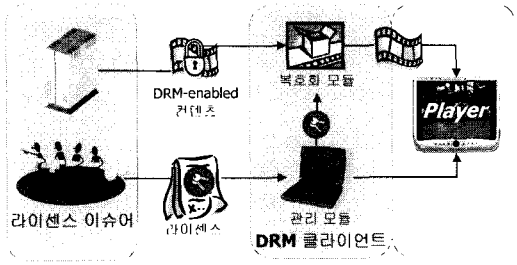
라이센스는 스트리밍 콘텐츠를 재생하는데 필요한 정보



〔그림 6〕 패키저 데이터 흐름도



〔그림 7〕 패키저 실행 화면



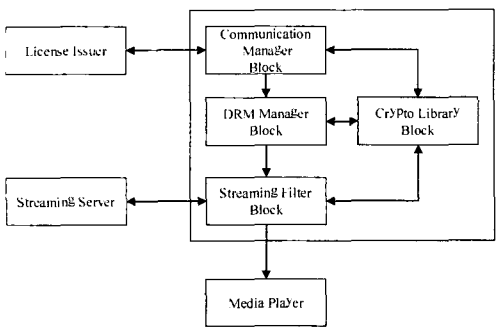
〔그림 8〕 라이센스 전달 및 스트리밍 서비스 흐름도

를 가지며 XML 형태로 작성되어 있다. 라이센스 이슈어는 콘텐츠 암호화에 사용된 암호화 키, 암호화 비율, 암호화 크기, 콘텐츠 ID, 미디어 종류, 플러그인 ID, 스트리밍 서버 URL 등의 메타데이터를 생성한다. DRM 클라이언트로부터 DRM 클라이언트의 공개키를 전달 받아 메타데이터를 암호화한 후 라이센스를 생성한다. 라이센스 이슈어는 클라이언트 시스템의 DRM 클라이언트를 호출하고 라이센스를 전달한다. 라이센스가 DRM 클라이언트의 공개키로 암호화되어 있기 때문에 DRM 클라이언트만이 복호화 할 수 있어 라이센스 이슈어와 DRM 클라이언트 사이의 안전한 라이센스 전달을 보장할 수 있다.

3. DRM 클라이언트

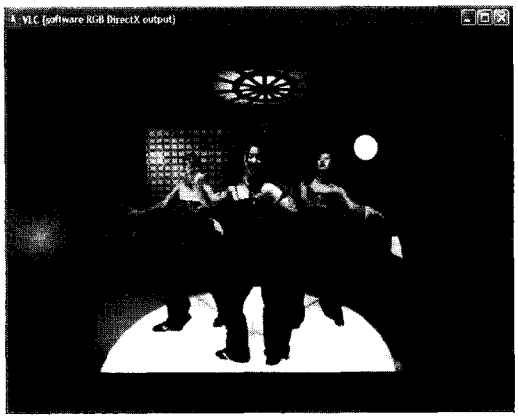
DRM 클라이언트는 라이센스 분석 및 파싱하여 DRM 정보를 처리하고, 스트리밍 서버로부터 스트리밍되는 콘텐츠를 실시간으로 복호화하고, 콘텐츠 플레이어를 제어하는 역할을 수행한다.

DRM 클라이언트와 라이센스 이슈어는 비대칭키 알고리즘을 기반으로 하여 통신 상에서 라이센스를 보호하며, 클라이언트 시스템 내에서 DRM 클라이언트만이 비밀키를 이용하여 공개키로 암호화된 암호키, 사용권한 등을 복호화하고 제어할 수 있도록 하여 중요한 정보가 누출되지 않도록 한다. DRM 클라이언트는 라이센스 이슈어로부터 전달 받은 라이센스를 인증한 후 그 내용을 분석하고 DRM 클라이언트의 공개키로 암호화된 것을 DRM 클라이언트의 비밀키로 복호화 한다. 라이센스에서 분석한 정보를 이용하여 스트리밍 URL을 알아내어 스트리밍 서비스를 요청하고 스트리밍 플레이어를 제어하며 스트리밍되는 암호화된 콘텐츠를 실시간으로 복호화 한다.



〔그림 9〕 DRM 클라이언트 구성도

클라이언트 사용자는 스트리밍 서비스는 암호화 되었거나 암호화되지 않았거나 같은 환경과 방법으로 서비스 받기를 원한다. DRM 클라이언트 사용자의 추가적인 작업이나 불편한 작업이 최소화가 될 수 있도록 한다. 본 논문에서 제안하는 스트리밍 필터를 이용한 방법은 기존의 스트리밍 플레이어에 대한 변경 없이 스트리밍 서비스를 할 수 있도록 하여 다양한 플레이어와 연동하여 스트리밍 서비스를 제공할 수 있다.



(라이센스가 없는 MPEG-2 콘텐츠 스트리밍 플레이)

(라이센스가 있는 MPEG-2 스트리밍 콘텐츠 플레이)

〔그림 10〕 라이센스가 있는 MPEG-2 스트리밍 콘텐츠 플레이와 라이센스가 없는 MPEG-2 콘텐츠 스트리밍 플레이 비교

스트리밍 필터는 스트리밍 서버와 플레이어 사이에 존재하는 프로그램이다. 클라이언트 시스템의 네트워크 프로토콜 상의 한 레이어(Layer)에 존재하게 되며 네트워크로 들어오는 스트리밍 패킷을 복호화하여 플레이어에게 전달한다.

Ⅳ. 결 론

본 논문은 스트리밍 서버의 성능을 보장하고 스트리밍 서버의 환경과 스트리밍 프로토콜에 영향을 주지 않으면서 스트리밍 콘텐츠를 안전하게 사용자에게 서비스할 수 있는 DRM 기반 콘텐츠 스트리밍 보호 시스템을 제안한다. 본 논문은 스트리밍 서버와 스트리밍 프로토콜에 영향을 주지 않도록 스트리밍 콘텐츠를 암호화하고 복호화에 필요한 정보를 라이센스를 기반으로 제공하여 넷트워크 패킷 캡쳐나 스트리밍 URL 캡쳐와 같은 불법적인 콘텐츠 사용을 방지하는데 근본적인 콘텐츠에 대한 보호 방법을 제공한다.

향후 무선 환경에서의 스트리밍 서비스를 위한 암호화 방법 및 DRM 연동에 대한 연구가 필요하다.

참 고 문 헌

[1] ISO/IEC 13818-1:2000 Information technology - Generic coding of moving pictures and associated audio information: Systems

[2] ISO/IEC 13818-2:2000 Information technology - Generic coding of moving pictures and associated audio information: Video

[3] ISO/IEC 13818-3:2000 Information technology - Generic coding of moving pictures and associated audio information: Audio

[4] ISO/IEC JTC 1/SC 29/WG 11 MPEG/N3939 Information technology- Multimedia framework(MPEG-21)- Part 1: Vision, Technologies and Strategy, January 2001

[5] Goichiro Hanaoka, Kazuto Ogawa, Itsuro Murota, Go Ohtake, Keigo Majima, Seiichi Gohshi, Kimiyuki Oyamada, Seiichi Namba, and Hideki Imai, "Managing Encryption and Key Publication Independentaly in Digital Rights Management Sytstems", IEICE TRANS. FUNDAMENTALS, VOL.E87-A, NO.1, JAN. 2004

[6] Junseok Lee, Seong Oun Hwang, Sang-Won Jeong, Ki Song Yoon, Chang Soon Park, and Jae-Cheol Ryou, "A DRM Framework for Distributing Digital Contents through the Internet", ETRI Journal, Vol. 25, pp.423-436, DEC. 2003

[7] Camp, L.J., "First principles of copyright for DRM design" Internet Computing, IEEE , Vol. 7, pp. 59-65, May-June 2003

[8] Deirdre K. Mulligan, John Han, Aaron J. Burstein, "How DRM-based content delivery systems disrupt expectations of personal use", Proceedings of the 2003 ACM workshop on Digital rights management, pp.77-88, October 2003

[9] Julie E. Cohen, "DRM and privacy", Communications of the ACM, Volume 46 Issue 4, April 2003

[10] Joshua Duhl, Susan KevorKian, "Understanding DRM Systems," IDC 2001

[11] Valimaki, M., Pitkanen, O., "Digital rights management on open and semi-open networks" Internet Applications, 2001. WIAPP 2001. Proceedings, pp.154 - 155, July 2001

[12] Frank Hartung, Friedhelm Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications" Communications Magazine, IEEE , Vol. 38 , pp.78-84, Nov. 2000

[13] Olin Sibert, "DigiBox: A Self-Protecting Container for Information Commerce", 1st USENIX Workshop on Electronic Commerce, 1995.

[14] SiRyong Yu, KyuHwan Jang, ByengWook Lee, JongIl Kim, HaeMook Jeong, "MPEG System," DaeyoungSa, 1997

〈著 者 紹 介〉

정 연 정 (Yeonjeong Jeong)

1994년 : 부산대학교 전자계산학과 (학사)
1996년 : 부산대학교 대학원 전자계산학과 (석사)
1996년~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 정보 보호, 저작권 보호

윤 기 송 (Kisong Yoon)

1984년 : 부산대학교 조선공학과(학사)
1988년 : City University of New York 전산학(석사)
1993년 : City University of New York 전산학(박사)
1993년~현재 : 한국전자통신연구원 책임연구원
〈관심분야〉 정보 보호, 저작권 보호, 분산 처리

류 재 철 (Jaecheol Ryu) 정회원

1985년 : 한양대학교 산업공학과(학사)
1988년 : Iowa State University 전산학과(석사)
1990년 : Northwestern University 전산학과(박사)
1991년~현재 : 충남대학교 정보통신공학부 교수
〈관심분야〉 정보 보호, 인터넷 보안